IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
BROWNSVILLE DIVISION

ROBERT L. COLLINS, *on behalf of himself and all others similarly situated,*	Civil Action No. 1:17-cv-187
Plaintiffs,	CLASS ACTION COMPLAINT
v.	JURY DEMAND REQUESTED
EQUIFAX, INC,	
Defendant.	

CLASS ACTION COMPLAINT

Plaintiff Robert L. Collins, on behalf of himself and all others similarly situated, alleges the following against Defendant Equifax, Inc., based upon personal knowledge and upon information and belief and the investigation and research of counsel:

NATURE OF THE CASE

1. Defendant Equifax, Inc. is a multi-billion dollar credit-reporting company. It is one of three nationwide credit-reporting agencies that is entrusted with personal credit data and financial information for millions of consumers in the United States, including information regarding their loans, credit cards, mortgages, employment histories, credit limits, child support obligations, consistency of rent and utilities payments, and other highly sensitive financial data. This information is used to calculate consumers' credit scores.

2. Equifax also collects and stores personal identifying information for millions of U.S. consumers such as Social Security numbers, address history, and other highly sensitive information. This personal and financial information is typically collected and stored by Equifax without the consumers' knowledge or prior consent.

3. On September 7, 2017, Equifax acknowledged that all of the above-mentioned personal data (collectively, "Consumer Data") was subject to a cybersecurity incident that impacted the Consumer Data of hundreds of millions of U.S. consumers (the "Security Breach"). Equifax claims that its investigation showed the unauthorized persons gained access to its U.S. website application for more than two months, from Mid-May through July 2017.

4. The number of persons impacted by this Security Breach is not yet fully clear, but is in the hundreds of millions of U.S. Consumers. Thus far, Equifax has admitted that 143 million consumers' Consumer Data was accessed, including names, birth dates, addresses, Social Security numbers, and driver's licenses numbers. Equifax has also admitted that unauthorized persons accessed the credit card numbers of approximately 209,000 U.S. consumers, and that the personal identifying information for approximately 182,000 U.S. consumers were accessed from certain credit dispute documents accessed during the breach.

5. Equifax discovered the unauthorized access on July 29, 2017, but inexplicably decided to withhold that information from the public for more than a month afterward. Equifax chose not to tell consumers that their highly sensitive personal and financial information—most of which, again, had been collected and stored without the consumers' knowledge or consent—had been stolen by unauthorized hackers. Equifax should have shared this disturbing information immediately after its discovery, so that millions of U.S. consumers would be aware of the new risks that the Security Breach had created, and of the urgent need to take immediate steps to protect themselves and their credit.

6. Instead of telling the public about the Security Breach during that month after discovering it, at least three Equifax executives instead spent that time lining their pockets, selling Equifax shares worth nearly $2 million shortly after the massive Security Breach.

7. Equifax could and should have taken steps to prevent this Security Breach, and certainly should have immediately advised the public promptly after it was discovered. Equifax knew about other recent cybersecurity threats, including breaches at its competitor Experian, and certainly knew that such breaches could result as foreseeable consequence of Equifax's inadequate data security and inadequate protection of the nation's Consumer Data it collected in the course of its business.

8. Equifax engaged in numerous harmful actions, including intentional, willful, reckless, and/or negligent acts and omissions that included failing to (a) take adequate and reasonable measures to protect Consumer Data, (b) take steps to prevent and stop the Security Breach from occurring in the first instance, (c) disclose to U.S. consumers that it did not have adequate security in place to safeguard Consumer Data, and (d) detect and disclose the Security Breach to the public in a timely manner.

9. Plaintiff has a substantial interest in safeguarding his own Consumer Data (which remains in Equifax's possession) and that of all class members from further breaches, as well as in seeking redress for the injury he and similarly situated consumers have suffered from the information stolen during the Security Breach.

10. Plaintiff's and class members' Consumer Data has been put in the hands of unknown criminals as result of the Security Breach. Plaintiff's and class members' injuries suffered, or likely to be suffered, as a result of the Security Breach include but are not limited to: (i) theft of their Consumer Data, including personal and financial information, (ii) costs to detect and prevent identify theft and/or unauthorized use of their financial records, (iii) loss of privacy, (iv) imminent injury from potential fraud and identify theft from the use of their Consumer Data by unauthorized persons, (v) sale of Plaintiff's and class members' Consumer Data on the black

market, (vi) costs associated with time spent addressing or attempting to remedy the present and likely future consequences of the Security Breach.

11. Plaintiff brings this as a national class action on behalf of more than 140 million consumers harmed by the Security Breach, Equifax's failure to adequately protect their Consumer Data, and Equifax's inexplicable delay in disclosing the Security Breach.

THE PARTIES

12. Plaintiff Robert L. Collins is an individual consumer residing in South Padre Island in the state of Texas. Plaintiff is a victim of the Security Breach.

13. Defendant Equifax, Inc. is a Georgia corporation with its headquarters and principal place of business in Atlanta, Georgia. Equifax may be served with service of process through its registered agent in Texas, Prentice-Hall Corporation System at its address of 211 E. 7th Street, Suite 620, Austin, Texas 78701.

JURISDICTION AND VENUE

14. This civil action asserts a claim for violation of the Fair Credit Reporting Act, 15 U.S.C. § 1681. Accordingly, this Court has subject matter jurisdiction over this civil action as it arises under the laws of the United States, 28 U.S.C. § 1331. The Court has jurisdiction over Plaintiff's remaining claims under 28 U.S.C. § 1367.

15. This Court also has subject matter jurisdiction over this civil action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) as at least some members of the proposed class (including Plaintiff) are citizens of different states than Equifax, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

16. This Court has personal jurisdiction over Equifax because Equifax has sufficient minimum contacts with Texas including the fact that it conducts business involving the personal

and financial information of millions of consumers in this jurisdiction (including Plaintiff's).

17. Venue is proper in the Southern District of Texas under 28 U.S.C § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District. Plaintiff resides in this District and Equifax conducts business with consumers, including Plaintiff, in this District and has caused injury to many more residents of this District.

FACTUAL BACKGROUND

18. The Equifax Security Breach is particularly distressing for Plaintiff and similarly situated U.S. consumers because consumers do not know what aspects of their Consumer Data is in Equifax's possession, much less what exactly was stolen. Indeed, many consumers may not even be aware that Equifax holds their Consumer Data. In contrast to many other firms that have experienced data breaches, consumers do not provide their information to Equifax of their own volition. Rather, Equifax obtains the highly sensitive Consumer Data by purchasing public data and by obtaining it from other companies—such as, for example, banks and credit card companies—who report on individual consumer' credit activity to Equifax.

19. Equifax identified a cybersecurity incident potentially impacting 143 million U.S. consumers on July 29, 2017.[1] This unauthorized access to Consumer Data occurred from mid-May through July 2017.

20. Equifax did not publicly disclose the Security Breach until September 7, 2017.

21. The information accessed primarily includes the Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers of millions of consumers. Unauthorized third party criminals also accessed credit card numbers for approximately 209,000

[1] These factual allegations are largely derived from information Equifax has provided on its public website. *See* https://www.equifaxsecurity2017.com/frequently-asked-questions/ (last accessed September 11, 2017).

U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers.

22. This personal Consumer Data will likely be sold and used by cybercriminals. Plaintiff and all similarly situated U.S. consumers will suffer imminent injury from the substantially increased risk of identify theft, fraud and misuse of their personal data because their Consumer Data is in the hands of cybercriminals who have – or will imminently – use the stolen Consumer Data to, among other things, open unauthorized accounts and lines of credit.

23. Equifax demonstrated its awareness and agreement that Plaintiff and the more than 143 million similarly situated U.S. consumers are in immediate need of credit monitoring services when it offered those consumers the option to enroll in TrustedID Premier. Due to overwhelming demand, many U.S. consumers must wait a week or more to enroll. Furthermore, the service will only last one year, which is woefully insufficient to secure Plaintiff's and class members' Consumer Data from the ongoing risk arising out of the Security Breach. Equifax even tried to prevent consumers from seeking legal relief relating to the Security Breach; consumers provided with the TrustedID Premier option had to agree to a fine print forced arbitration clause. Equifax attempted to "clarify" its position on that clause's applicability following criticism by the media and the Attorney General of New York. However, many consumers were confused, and remain confused, by Equifax's highly improper tactics designed to limit its massive exposure.

24. Equifax owed a legal duty to consumers like Plaintiff to use reasonable care to protect their credit and personal Consumer Data from unauthorized access by third parties. Equifax knew that its failure to protect U.S. consumers' credit and personal Consumer Data from unauthorized access by cybercriminals would create serious, imminent risks of harm, both

immediately and for many years.

25. Equifax willfully, recklessly, or negligently failed to maintain adequate technological and cybersecurity safeguards to protect Plaintiff's information from vulnerability to access by unauthorized persons. Equifax could have, but chose not to, spend additional money to protect the nation's Consumer Data against cyber attacks. Equifax elected to cut corners and save money at the expense of U.S. consumers' security.

26. Equifax executives also lined their pockets in the wake of the Security Breach. Three executives sold Equifax shares worth nearly $2 million shortly after the massive Security Breach, and long before Equifax announced the Security Breach to the public. Chief Financial Officer John Gamble sold shares worth nearly $950,000 on August 1. Equifax president for U.S. information solutions, sold shares worth about $685,000 on August 1 as well. Rodolfo Ploder, president of workforce solutions, sold stock for just more than $250,000 on August 2. None of these transactions are listed on filings with SEC as being part of 10b5-1 scheduled trading plans.

27. Plaintiff has suffered actual damages from the substantially increased risk of future identify theft, fraud, and misuse of their Consumer Data in the hands of criminals.

28. Plaintiff has also suffered actual injury in the form of damage to and decreased value of their Consumer Data. Consumer Data is intangible property that Plaintiff and other similarly situated consumers entrusted to Equifax, and that Equifax allowed to be compromised through its willful, reckless and negligent conduct that led to the Security Breach.

29. Consumer Data is highly valued on criminal black markets that trade and sell stolen information. Criminals then use the stolen Consumer Data to make charges on existing credit card accounts, clone debit and credit cards, and take out new loans in a victim's name.

30. Identity thieves can also use Consumer Data such as Plaintiff's in the course of a

number of crimes, including: obtaining a driver's license in another person's name, immigration fraud, government benefits' fraud, and filing fraudulent tax returns to obtain a refund.

31. In addition to any fraudulent use of their own Consumer Data, Plaintiff and class members now face years if not decades of having to constantly surveil and monitor their financial records and personal records.

32. Despite this serious risk that Equifax knew existed, Equifax did not take adequate measures to secure the privacy and safety of Consumer Data. Equifax's failure to implement adequate security measures against cyber attack was willful, reckless, and/or negligent.

33. Equifax had the means to remedy the deficiencies in their security systems, establish adequate security guidelines, and adopt approved security measures. Had Equifax done so, it could have prevented the Security Breach. Equifax's failures are the actual and proximate cause of the damages Plaintiff has suffered and will continue to suffer.

CLASS ALLEGATIONS

34. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff brings these claims and seeks relief on behalf of all similarly situated U.S. consumers, and will seek to certify a "Nationwide Class" consisting of:

> All United States residents whose personal financial, credit, and identifying information was accessed by third parties as a result of the Equifax data security breach that Equifax announced as having taken place during the months of May through July of 2017.

35. Pursuant to Federal Rule of Civil Procedure 23, and in the alternative, Plaintiff brings these claims on behalf of all similarly situated Texas consumers, and will seek to certify a "Texas Class" consisting of:

> All Texas residents whose personal financial, credit, and identifying information was accessed by third parties as a result of the Equifax data security breach that Equifax announced as having taken place during the months of May through July

of 2017.

36. The Nationwide Class and Texas Class exclude the Defendant, any affiliated entities, its officers and directors, its employees, the judge to whom this case is assigned, and court staff, as well as their immediate families.

37. The members of the Nationwide Class and Texas Class are so numerous that joinder of all members is impracticable. The Nationwide Class will include as many as 143 million U.S. consumers. While the exact number of Texas Class members is unknown to Plaintiff at this time, Plaintiff believes that there are likely millions of members of the proposed class.

38. Plaintiff's claims are typical of the claims of the members of the Nationwide and Texas Classes, as all members of the Class are similarly affected by Equifax's wrongful conduct in violation of federal law and as well as by Equifax's negligence. All Class members will suffer damages relating to the Security Breach, including the costs to monitor and repair their credit through a third-party service.

39. Plaintiff will fairly and adequately protect the interests of the members of the Classes and has retained counsel competent and experienced in class action litigation.

40. Common questions of law and fact exist as to all members of the Classes and predominate over any questions solely affecting individual members of the Classes. Questions of law and fact common to the Classes include, among other things, (a) whether Equifax was negligent in failing to implement adequate security procedures and practices to protect Consumer Data; (b) whether Equifax's failure to implement adequate security procedures and practices was the actual and/or proximate cause of the Security Breach; (c) whether Equifax knew or should have known that their security procedures and practices were insufficient to avoid the Security

Breach; (d) whether Plaintiff and class members were injured as the result of Equifax's failure to reasonably protect the Consumer Data; and (e) whether Plaintiff and class members are entitled to relief and the type of relief to which they are entitled, such as damages to cover the costs associated with appropriate credit monitoring protection to mitigate against further consequential damages.

41. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. The damages suffered by Plaintiff and class members may be small relative to the burden and expense required to litigate their individual claims against a massive entity with substantial resources like Equifax. As such, individual litigation to redress Equifax's wrongful conduct would be impracticable. Individual litigation by potentially millions of U.S. consumers would also be inefficient and unnecessarily burden the courts.

42. Plaintiff reserves the right to amend or modify the class definitions after he has had the opportunity to engage in discovery.

CAUSES OF ACTION

COUNT 1: Negligence

43. Plaintiff repeats and realleges every allegation above as if fully set forth herein.

44. As described herein Equifax accepted, bought, and stored Consumer Data belonging to Plaintiff and the class members. Equifax thus undertook and assumed a duty to Plaintiff and the class members to exercise reasonable care to secure and safeguard their Consumer Data using commercially reasonable means.

45. The Consumer Data was the foreseeable and probable target of attempted cyber attacks, especially in light of recent security breaches at other firms. As such, Equifax owed Plaintiff and class member a duty of care not to subject the Consumer Data (and in turn Plaintiff

and class members) to an unreasonable risk of harm.

46. Equifax knew or should have known the intrinsic security risks with obtaining and storing Consumer Data.

47. Equifax knew or should have known that its data and security systems did not adequately protect Plaintiff's and class members' Consumer Data.

48. Equifax breached its duties to Plaintiff and class members by failing to provide adequate security measures to protect the Consumer Data of Plaintiff and class members.

49. Equifax breached its duties to Plaintiff and class members by failing to (a) take adequate and reasonable measures to protect Consumer Data, (b) detect and disclose the Security Breach in a timely manner, (c) take steps to prevent and stop the Security Breach from occurring in the first instance, and (d) disclose to U.S. consumers that it did not have adequate security in place to safeguard Consumer Data.

50. Equifax had independent duties under state and federal law, including the Fair Credit Reporting Act and Federal Trade Commission Act, to reasonably safeguard Plaintiff's and class members' Consumer Data and promptly notify them about the Security Breach. Equifax breached these duties as well.

51. As a direct and proximate cause of Equifax's unlawful conduct, Plaintiff and the class suffered damages including but not limited to:

a. The cost of third-party monitoring services to detect unauthorized use of Plaintiff's and class members' Consumer Data;

b. Potential adverse consequences of identity theft or other privacy losses; and

c. Other economic damages not yet identified and that may not be capable of identification for many years.

COUNT 2: Willful Violation of the Fair Credit Reporting Act ("FCRA")

52. Plaintiff repeats and realleges every allegation as if fully set forth herein.

53. Plaintiff and class members are consumers whose rights are protected by FCRA, 15 U.S.C. § 1681a(c).

54. Equifax is a "consumer reporting agency" as defined in FRCA, 15 U.S.C. § 1681a(f), as it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, for monetary fees.

55. Equifax is required by FCRA, 15 U.S.C. § 1681e(a), to maintain reasonable procedures to limit the furnishing of customer reports for limited purposes. Equifax may only furnish a consumer report under limited circumstances as set forth in 15 U.S.C. § 1681b. None of these purposes include allows Equifax to furnish consumer reports or Consumer Data to unauthorized persons, entities or cybercriminals such as those who accessed Plaintiff's and class members' Consumer Data.

56. Equifax violated 15 U.S.C. § 1681b by furnishing consumer reports to unauthorized persons, entities or cybercriminals as set forth in detail above.

57. Equifax was aware that the Federal Trade Commission ("FTC") has pursued enforcement actions against other consumer reporting agencies under FCRA for failing to "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by" FCRA, in connection with other agencies' security breaches.

58. Equifax willfully violated FCRA §§ 1681b and 1681e(a) by intentionally failing to maintain adequate security measures and procedures to limit the furnishing of consumer reports outside the statutorily permissible purposes. Equifax was well aware of the importance of

security to prevent data breaches, and despite representing itself as having sufficient security measures in place, Equifax willfully failed to take reasonable steps to prevent the Security Breach.

59. Equifax also acted willfully insofar as it intentionally ignored the FTC's regulations implementing FCRA and outlining consumer reporting agencies' obligations to implement data security and avoid data security breaches. Equifax knew or should have known about these requirements and obligations.

60. Despite knowing of these requirements and obligations, Equifax consciously chose to disregard its duties to consumers relating to data security. Equifax's willful actions deprived Plaintiff and class members of their rights under FCRA.

61. Equifax acted willfully in providing a means for unauthorized persons and cybercriminals to obtain and misuse Plaintiff's and class members' Consumer Data for no permissible purposes under FCRA.

62. Plaintiff and class members have been damaged by Equifax's willful violation of FCRA. Plaintiff and class members therefore are entitled to recover all actual damages suffered "or damages of not less than $100 and not more than $1,000" per class member, plus interest, punitive damages, attorney's fees and costs. 15 U.S.C. § 1681n(a)(1)(A), (2) and (3).

COUNT 3: Negligent Violation of the Fair Credit Reporting Act ("FCRA")

63. Plaintiff repeats and realleges every allegation as if fully set forth herein.

64. Equifax acted negligently in failing to maintain adequate security measures and procedures to limit the furnishing of consumer reports outside the statutorily permissible purposes. Equifax's negligence is shown by its awareness of the importance of security to prevent data breaches. Equifax negligently failed to take such steps causing the Security Breach.

65. Equifax's negligent conduct provided a means for unauthorized persons and cybercriminals to obtain Plaintiff's and class members' Consumer Data and consumer reports for only impermissible purposes.

66. Plaintiff and class members have been damaged by Equifax's negligent violation of FCRA. Plaintiff and class members therefore are entitled to recover all actual damages they have suffered "or damages of not less than $100 and not more than $1,000" per class member, plus interest, punitive damages, attorney's fees and costs. 15 U.S.C. § 1681o(a)(1) and (2).

67. Plaintiff and class members are also entitled to recover their costs of the action as well as reasonable attorneys' fees pursuant to 15 U.S.C. § 1681o(a)(2).

COUNT 4: Declaratory Judgment

68. Plaintiff repeats and realleges every allegation as if fully set forth herein.

69. Equifax continues to possess Plaintiff's and other proposed class members' Consumer Data. Indeed, Equifax holds a tremendous amount of Consumer Data for nearly every adult in the United States.

70. Given Equifax's position as a holder of so much Consumer Data for persons nationwide, it owes a special duty of care to safeguard said Consumer Data, both to protect individual consumers as well as to prevent massive financial and credit disruptions to the public at large.

71. Equifax has failed to provide adequate data security to protect Plaintiff's and class members' Consumer Data, as manifested by the Security Breach. Equifax has not taken meaningful steps to remedy the vulnerabilities in its computer data and security systems that led to the Security Breach and could lead to further security breaches.

72. As such, Equifax continues to breach its duty to Plaintiff and all class members to

prevent massive injuries from security breaches.

73. An order from this Court declaring that Equifax continues to breach its high duty of care to Plaintiff and all class members is necessary to compel Equifax to adequately protect the incredibly sensitive information it holds.

74. Plaintiff therefore seeks a declaration that:

a. Equifax's current data security measures do not satisfy its duty of care to all persons whose Customer Data it possesses; and

b. Equifax must identify, implement, and maintain additional reasonable security measures to protect Consumer Data, with said measures to be determined by the Court after assessing the facts to be obtained in discovery that demonstrate the full extent of the weaknesses in Equifax's current data security systems that were exposed and exploited by the Security Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief and judgment, as follows:

A. Determining that this action is proper as a class action, designating Plaintiff as class representative under Rule 23 of the Federal Rules of Civil Procedure and Plaintiff's counsel as Class counsel;

B. Awarding compensatory damages in favor of Plaintiff and the other class members against Equifax for all damages sustained as a result of its wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Awarding Plaintiff and the Classes punitive damages and their reasonable costs and expenses incurred in this action, including counsel fees and expert fees as allowable by law;

D. Declaring that Equifax's current data security measures do not satisfy its duty of

care to all persons whose Customer Data it possesses;

E. Declaring that Equifax must identify, implement, and maintain additional reasonable security measures needed to protect the Consumer data of all United States residents and prevent further massive injury to the public, with said measures to be determined by the Court; and

F. Such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues triable by jury.

Dated: September 11, 2017

Respectfully submitted,

EDISON, MCDOWELL & HETHERINGTON LLP

By: _____

Thomas FA Hetherington
State Bar No. 24007359
Federal ID No. 23102
Kendall J. Burr
State Bar No. 24067533
Federal ID No. 1057156
First City Tower
1001 Fannin Street, Ste. 2700
Houston, Texas 77002
Telephone: (713) 337-5580
Fax: (713) 337-8850
E-Mail: tom.hetherington@emhllp.com
kendall.burr@emhllp.com

CHANDLER MCNULTY, LLP

Troy D. Chandler*
6575 West Loop South, Ste. 605
Houston, TX 77401
Telephone: 713-997-8310
E-Mail: troy@chandlermcnulty.com

**Pro Hac Vice Application Forthcoming*

ATTORNEYS FOR PLAINTIFF
ROBERT L. COLLINS AND THE PROPOSED
CLASSES